



UT VOCE ITA VITA

EXETER CATHEDRAL SCHOOL

Nursery | Pre-Prep | Prep

E – SAFETY POLICY – (P12)

Review period: Annual

Reviewed by: SLT **Date:** 27/11/2017

Oversight by: Academic Subcommittee

Next review due: Nov 2018

This policy and guidance is applicable to all those involved in the provision of e-based education and resources at Exeter Cathedral School and to all persons with access to or who are users of school's ICT systems. This policy should be read in conjunction with the school's policy on the Acceptable Use of ICT Systems and Mobile Devices.

1 Objectives

- To ensure that pupils are appropriately supervised during school activities
- To promote responsible behaviour with regard to e-based activities
- To take account of legislative guidance

2 Guidance

2.1 The Assistant Head will act as E- Safety Coordinator and will:

- be responsible for the implementation of this policy compile logs of e-safety incidents
- compile logs of e-safety incidents
- report to the Headmaster and Bursar on recorded incidents
- ensure that staff are aware of this guidance
- provide / arrange for staff training
- liaise with school technical staff
- liaise with the Headmaster on any investigation and action in relation to e-incidents
- advise on e-safety policy review and development

2.2 The Bursar will act as the ICT (Systems) Coordinator and will:

- be responsible for the IT infrastructure and that it is not open to misuse or malicious attack
- ensure that users may only access the networks and devices through an enforced password protection policy
- keep up to date with e-safety technical information in order to carry out their role
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse
- implement any agreed monitoring software / systems

2.3 Teaching and Support Staff will:

- maintain awareness of school e-safety policies and practices
- report any suspected misuse or problem to the Headmaster or E-Safety Coordinator

Exeter Cathedral School • The Chantry • Palace Gate • Exeter • EX1 1HX

Telephone: 01392 255298 • Website: www.exetercs.org • Email: reception@exetercs.org



- ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems
- where relevant ensure that e-safety is recognised in teaching activities and curriculum delivery
- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies (including mobile devices, cameras etc during school activities
- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

2.4 Child Protection

Those responsible for the oversight of Safeguarding (Child Protection) should be trained in e-safety issues and aware of the implications that may arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate contact on-line with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

2.5 Pupils

With the support and guidance of teaching staff:

- are responsible for using school digital technology systems in accordance with the school acceptable use policy
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying
- will understand that the e-safety policy will include actions outside of school where related to school activities

2.6 Parents / Carers

- will be advised of e-safety policies through parents evenings, newsletters, letters and the school website etc
- will be encouraged to support the school in the promotion of good e-safety practice
- should follow school guidelines on:
 - digital and video images taken at school events
 - access to parents sections of the school website and MIS and their children's records
 - their children's personal devices in the school (where this is permitted)

2.7 Community Users / Contractors



Where such groups have access to school networks / devices, they will be expected to provide signed acceptance to abide by school e-safety policies and procedures.

Legal Requirements & Education Standards

References:

Handbook for the Inspection of Schools - The Regulatory Requirements, Part 3 (www.isi.net)

Reference Guide to the key standards in each type of social care service inspected by Ofsted (www.ofsted.gov.uk)

[Health and Safety at Work" Section H of the ISBA Model Staff Handbook,](#)

[Health and Safety and Welfare at Work" Chapter N of the ISBA Bursar's Guide](#)

[Insurance" Chapter K of the Bursar's Guide by HSBC Insurance Brokers Ltd](#)

UK Council for Child Internet Safety (www.education.gov.uk/ukccis)

Cyber-bullying.org (www.cyberbullying.org)

Department for Education "Safer Working Practice for Adults who Work with Children and Young People" (www.education.gov.uk)